Physical-Layer Security With Full-Duplex Transceivers and Multiuser Receiver at Eve

Nurul Huda Mahmood, *Member, IEEE*, Imran Shafique Ansari, *Member, IEEE*, Petar Popovski, *Fellow, IEEE*, Preben Mogensen, and Khalid A. Qaraqe, *Senior Member, IEEE*

***Abstract*— Full-duplex communication enables simultaneous transmission from both ends of a communication link, thereby promising significant performance gains. Generally, it has been shown that the throughput and delay gains of full-duplex communication are somewhat limited in realistic network settings, leading researchers to study other possible applications that can accord higher gains. The potential of full-duplex communication in improving the physical-layer security of a communication link is investigated in this contribution. We specifically present a thorough analysis of the achievable ergodic secrecy rate and the secrecy degrees of freedom with full-duplex communication in the presence of a half-duplex eavesdropper node, with both single-user decoding and multi-user decoding capabilities. For the latter case, an eavesdropper with successive interference cancellation and joint decoding capabilities is assumed. Irrespective of the eavesdropper capabilities and channel strengths, the ergodic secrecy rate with full-duplex communication is found to grow linearly with the log of the direct channel signal-to-noise-ratio (SNR) as opposed to the flattened out secrecy rate with conventional half-duplex communication. Consequently, the secrecy degrees of freedom with full-duplex is shown to be *two* as opposed to that of *zero* in half-duplex mode.**

***Index Terms*— Full-duplex, 5G, Physical-layer security, secrecy degrees of freedom, interference cancellation receivers, joint decoding.**

I. Introduction

HISTORICALLY, full-duplex communication, i.e. simultaneous transmission and reception on the same radio resource, had been considered impractical due to the overwhelming loopback interference from the transmission-end at the co-located receiver. Recent advances in self-interference cancellation (SIC) allow suppressing this loopback interference to within tolerable limits, thereby making full-duplex (FD) communication appealing with viable cost. Ideally, FD communication has the potential to provide a 100% throughput gain over conventional half-duplex (HD) transmissions, making it a candidate technology component in the design of a novel fifth Generation (5G) radio access technology [1]–[3].

Until recently, most studies on FD communication have investigated its potential in according a throughput gain [3]–[8], and/or improving the transmission latency [9], [10]. It has been shown that the expected throughput gains are conditioned on three strong assumptions [11], namely i) perfect SIC, ii) available traffic at both ends to exploit the arising transmission opportunities, and iii) similar levels of network interference with FD and HD transmissions. Simultaneous transmission from both ends leads to higher inter-cell interference (ICI) for a network of FD nodes compared to conventional HD nodes [3], [6]. Such increased ICI, along with any residual self interference power, results in a reduction of the possible throughput gains. Additionally considering a practical downlink heavy traffic profile limits the instances where the simultaneous transmission/reception capabilities of FD communication can be utilized, resulting in a further reduction of the throughput gains [10], [11].

Due to the somewhat limited throughput gain and latency reduction, other potential applications of FD communication have recently been investigated. The requirement of having symmetric traffic in order to exploit FD opportunities have lead to studying FD transmission for scenarios with symmetric traffic profile, such as backhaul communication [12], [13]. Relays are also envisioned as a potential application area for FD communication. The use of relays in multi-user FD communication systems is considered as an effective approach to improve spectral efficiency and expand its coverage [14], [15]. A relay-aided interference cancellation technique was proposed for a FD relay wireless networks in [14]; whereas the authors in [15] have proposed a two-timeslot two-way FD relaying scheme for 5G wireless communication systems. In addition, some advances in throughput analysis and optimization of wirelessly powered multi-antenna FD relay systems were demonstrated in [16].

The broadcast nature of wireless transmission makes it vulnerable to be eavesdropped and raises potential security concerns. Information-theoretic physical-layer security approach focuses on the inherent capacity of the propagation channel to provide security in the physical-layer itself [17, and references therein]. Cooperative transmission via relays has been proposed as an effective physical-layer security scheme [18]. The performance of secure FD relaying has recently been analyzed for single hop [19] and multi-hop [20] relays. However, reference [19] assumes non-negativity of the secrecy rate (which is valid only when the direct channel is much stronger than

Manuscript received October 18, 2016; revised March 14, 2017 and May 11, 2017; accepted May 30, 2017. Date of publication June 9, 2017; date of current version October 16, 2017. The associate editor coordinating the review of this paper and approving it for publication was M. Tao. *(Corresponding author: Nurul Huda Mahmood.)*

N. H. Mahmood and P. Popovski are with the Department of Electronic Systems, Aalborg University, 9220 Aalborg, Denmark (e-mail: fuadnh@ieee.org).

I. S. Ansari and K. A. Qaraqe are with the Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Education City, Doha, Qatar.

P. Mogensen is with the Department of Electronic Systems, Aalborg University, Aalborg, Denmark, and also with Nokia Bell Labs, 9220 Aalborg, Denmark.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2017.2713816

the eavesdropper channel), whereas reference [20] assumes perfect SIC; both being too optimistic as assumptions. Rather than either HD or FD mode, a new hybrid FD/HD relay selection technique to improve the physical-layer security has been developed in [21]. The authors in [22] have investigated the secrecy performance of FD relay networks demonstrating it to have a better secrecy performance than HD relay networks in scenarios where self-interference can be well suppressed. They further proposed a FD jamming relay network wherein the relay nodes transmit jamming signals simultaneously as it receives the data from the source.

Physical-layer security with FD nodes for non-cooperative communication has started gaining attention as well. A transmit beamforming scheme for a full-duplex base station (FD-BS) considering physical-layer security guarantee for the system with multiple passive eavesdroppers is proposed in [23]. On the other hand, [24] investigates the potential of using FD jamming receivers to improve physical-layer secrecy and robustness without the aid of external relays. However, both of these contributions focus on developing a transmission scheme to optimize the secrecy rate with simplistic assumptions limiting the applicability in realistic scenarios (e.g., strict achievability of positive secrecy rate as in [19]).

The authors in [25] have designed a joint information and jamming beamformer to ensure security at both the ends for a FD-BS. Reference [26] considers a joint beamforming and power optimization problem for multi-antenna full-duplex transmission systems. The authors propose to utilize information bearing signals to additionally act as artificial noise against eavesdroppers, and show that the overall throughput can be improved while simultaneously maintaining the desired secrecy and quality of service levels. On the other hand, the network requirements for a FD-BS are addressed to secure the information being shared in a simultaneous information and power transfer energy harvesting nodes in [27]. Furthermore, an underlay cognitive radio system is considered in [28] wherein the secondary transmitter sends information to a FD receiver node in presence of an eavesdropper. The receiver node is equipped with a power-splitter architecture, allowing it to receive information as well as energy from the source. This received energy is utilized to transmit jamming signals to deteriorate eavesdropper's decoding capacity. The work in [29] assumes a FD wiretap channel in the presence of an eavesdropper and imperfect channel state information, and proposes techniques to maximize the achievable sum secrecy rate.

A. Key Contributions

The secrecy potential of FD communication, expressed in terms of the ergodic secrecy rate and the secrecy degrees of freedom, is thoroughly analyzed in this contribution; and compared against that of an equivalent HD links. This article extends the state-of-the-art on the physical-layer security potential of FD communication by specifically relaxing the strictly positive secrecy rate constraint and considering non-ideal SIC. Both, a single-user decoding Eve (SU-Eve) with passive linear receivers, and a multi-user decoding Eve (MU-Eve) with successive interference cancellation (IC) and multiple access channel (MAC) joint decoding (JD) capabilities, are both considered. In particular, the main contributions of this paper in specific terms are[1]

- We present a closed form expression for the ergodic secrecy rate of FD communication considering different capabilities at Eve and non-ideal SIC,
- the strictly positive secrecy rate assumption is relaxed by allowing unconstrained eavesdropper channel strength,
- the secrecy degrees of freedom of the considered scenarios are characterized, and
- applications of the findings in emerging 5G networks are discussed.

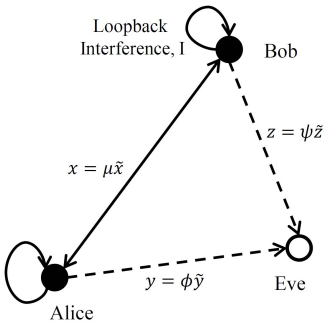


Fig. 1. System Model showing the considered FD transceiver pair in the presence of Eve.

B. Paper Organization

Section II introduces the system model. Closed form expressions for the ergodic secrecy rate upper bound, and the achievable secrecy rate gap with respect to the upper bound when considering Eve equipped with IC and MAC JD capabilities are analyzed in Section III. The secrecy degrees of freedom is then characterized in Section IV. Section V discusses application of the derived findings in emerging 5G networks. Finally, numerical results are presented in Section VI, followed by closing remarks and future outlook in Section VII.

II. System Model

Information-theoretic security characterizes the fundamental ability of the physical-layer to provide confidentiality. Let us consider a single small cell with an active transceiver pair, *Alice* and *Bob*, in the presence of *Eve* - an eavesdropper, as shown in Figure 1. Alice intends to transmit an encoded message W of coding block length n with rate R to Bob. The rate R is said to be *achievable with perfect secrecy* with respect to Eve if, as $n \to \infty$: (a) the probability of decoding error at Bob vanishes, and (b) the uncertainty of the message W as observed at Eve approaches the entropy of the message itself [17], [32]. Following [17] and [33], we consider the secrecy capacity of the Gaussian wiretap channel defined as difference between the source-destination and the source-eavesdropper rate to be the achievable secrecy rate.

An isolated cell is considered in order to focus the analysis on FD communication. Each node in the transceiver pair can

[1]Partial results of this work are presented in [30] and [31].

operate in either FD or HD mode. When operating in FD mode, the appropriate SIC schemes are assumed to limit the loopback self interference power to within tolerable limits. The random variables $\Pi \in \{X, Y, Z\}$ in Figure 1 denote the random signal-to-noise-ratios (SNR) of the respective channels among Alice, Bob, and Eve. The realizations $\varphi \in \{x, y, z\}$ of the respective random variable (rv) Π is represented as $\varphi = \bar{\varphi}\tilde{\varphi}$, with $\bar{\varphi} \in \{\mu, \phi, \psi\}$ being the mean and $\tilde{\varphi}$ a unit mean rv similarly distributed as φ.

A. Signal Model

1) Desired Signal Power: With FD communication, the desired signal to interference plus noise ratio (SINR) at Bob (and Alice) is denoted as

$$\gamma_{FD} = \frac{X}{I+1}, \tag{1}$$

where I denotes the noise-normalized residual self interference power after SIC at the receiver end. In the case of HD nodes $I = 0$, and the SINR is simply given by the SNR, i.e., $\gamma_{HD} = X$.

Generally, the desired Alice-Bob link is part of the same system and hence system designers have more information about, and control over, this link. The Nakagami-m fading distribution, which is a general fading distribution that includes a wide range of other distributions as special cases via its shape parameter m [34], is therefore adopted to model the desired signal amplitude. The SNR X is correspondingly distributed according to the following gamma distribution [34]

$$f_X(x; m, \mu) = \frac{m^m x^{m-1}}{\mu^m \Gamma(m)} \exp\left(-\frac{mx}{\mu}\right), \tag{2}$$

where the gamma distribution is characterized by the parameter m and the mean SNR μ, and $\Gamma(m) \triangleq \int_0^\infty t^{m-1}\exp(-t)\,\mathrm{d}t$ is the Gamma function.

The cumulative distribution function (CDF) of X, defined as $F_X(x) = \int_0^x f_X(t)\,\mathrm{d}t$ is given by

$$F_X(x; m, \mu) = \frac{\gamma\left(m, \frac{mx}{\mu}\right)}{\Gamma(m)}, \tag{3}$$

where $\gamma\ (m, x) \triangleq \int_0^x t^{m-1}\exp(-t)\,\mathrm{d}t$ is the lower incomplete Gamma function [35, 6.5.2].

2) Signal Power at the Eavesdropper Node: Without loss of generality, we assume Alice to be the transmitting node in HD scenario. The eavesdropped message at Eve is received with the SNR $\beta_{HD} = Y$. In contrast, Alice and Bob transmit simultaneously in FD mode, resulting in an additional source of interference at Eve. The resulting SINR of the eavesdropped message at Eve from Alice and Bob are respectively given by

$$\beta_a = \frac{Y}{Z+1}, \quad \text{and} \quad \beta_b = \frac{Z}{Y+1}. \tag{4}$$

Since the eavesdropper is usually an external node to the Alice-Bob system with more uncertainty about its location, the signal amplitude at Eve is assumed to follow the widely adopted Rayleigh fading distribution. The SNR Y (and Z) with mean $\phi(\psi)$ are correspondingly distributed according to the following exponential distributions [34]

$$f_Y(y) = \frac{1}{\phi}\exp\left(-\frac{y}{\phi}\right), \quad \text{and } f_Z(z) = \frac{1}{\psi}\exp\left(-\frac{z}{\psi}\right). \tag{5}$$

a) The distribution of β: To derive the distribution of β,[2] we introduce the variable $u = \frac{y}{z+1}$, and marginalize over the rv z in order to obtain $f_\beta(u|z) = f_Y(y(u))\frac{\mathrm{d}y}{\mathrm{d}u}$. The desired distribution of β is thereafter obtained as $f_\beta(u) = \mathbb{E}_z[f_\beta(u|z)] = \exp\left(-\frac{u}{\phi}\right)/\phi\mathbb{E}_z\left[(z+1)\exp\left(-\frac{uz}{\phi}\right)\right]$, where $\mathbb{E}[\cdot]$ is the expectation operator. Following some algebraic manipulations, the probability density function (PDF) is derived as

$$f_\beta(u) = \frac{\exp(-u/\phi)}{u\psi + \phi}\left[\frac{\phi\psi}{u\psi+\phi} + 1\right]. \tag{6}$$

On a similar note, the CDF of β defined as $F_\beta(u) = \int_0^u f_\beta(t)\,\mathrm{d}t$ evaluates to

$$F_\beta(u) = 1 - \frac{\exp(-u/\phi)}{1 + u\frac{\psi}{\phi}}. \tag{7}$$

For the special case when Eve is equidistant from Alice and Bob (i.e. $\phi = \psi$), the PDF and the CDF can respectively be further simplified as

$$\begin{aligned} f_\beta(u) &= \frac{\exp(-u/\phi)}{1+u}\left[\frac{1}{1+u} + \frac{1}{\phi}\right], \\ F_\beta(u) &= 1 - \frac{\exp(-u/\phi)}{1+u}. \end{aligned} \tag{8}$$

B. Achievable Secrecy Rate

1) Secrecy Rate With HD: Let us define the function $\mathcal{C}(x) = \log_2(1+x)$. Assuming the maximal additive white Gaussian noise (AWGN) rate can be achieved at every resource slot, the desired achievable rate between Alice and Bob is $R_x = \mathcal{C}(x)$, while the unwanted eavesdropped rate at Eve is $R_y = \mathcal{C}(y)$. Following the definition of secrecy rate as the strictly positive difference between the desired rate and the eavesdropped rate, the instantaneous secrecy rate in HD mode is given by

$$\begin{aligned} S_{HD} &= \max\left\{R_x - R_y, 0\right\} \\ &= \begin{cases} \mathcal{C}(x) - \mathcal{C}(y) & \text{when } x > y \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{9}$$

2) Secrecy Rate With FD: Alice and Bob can communicate simultaneously with each other when both are equipped with FD nodes, with both transmissions subject to potential overhearing by Eve. The achievable rate between Alice and Bob can be expressed as $R_{ab} = \mathcal{C}(\gamma_{FD})$, where γ_{FD} is the SINR in FD mode as given by Eq. (1). Similarly, the achievable rate at Eve considering the transmission from Alice to Bob is $R_{ae} = \mathcal{C}(\beta_a)$ with β_a given by Eq. (4). The instantaneous secrecy rate of the Alice to Bob link with FD transmissions is then given by

$$S_{FD,a} = \begin{cases} \mathcal{C}(\gamma_{FD}) - \mathcal{C}(\beta_a) & \text{when } \gamma_{FD} > \beta_a \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

[2]The index $\in \{a, b\}$ is henceforth dropped as the usage is clear from the context.

On a similar note, the instantaneous secrecy rate of the reverse Bob to Alice link with FD transmissions is $S_{FD,b} = \max\{R_{ab} - R_{be}, 0\}$, where $R_{be} = \mathcal{C}(\beta_b)$. Finally, the instantaneous secrecy rate of the considered system with FD communication can be expressed as $S_{FD} = S_{FD,a} + S_{FD,b}$.

C. Secrecy Degrees of Freedom

The degrees of freedom of a wireless link is an indication of the capacity pre-log factor in the capacity computation, and is an important information-theoretic measure [17], [36]. Being a difference of two achievable rates, the achievable secrecy rate easily lends itself to degrees of freedom analysis. More specifically, the secrecy degrees of freedom (sdof) region is a characterization of the high SNR behaviour of the secrecy capacity. Following [17] and [37], we define the sdof with the ratios $\eta_\phi \triangleq \frac{\mu}{\phi}$ and $\eta_\psi \triangleq \frac{\mu}{\psi}$ fixed as

$$d_\vartheta = \lim_{\mu\to\infty} \sup \frac{S_\vartheta}{\log \mu}, \tag{11}$$

where $\vartheta \in \{HD, FD\}$ is the transmission mode.

III. Achievable Secrecy Rate Analysis

The first part of this section considers a SU-Eve equipped with a linear receiver, which represents an upper bound on the achievable secrecy rate with FD communication. A more advanced receiver at Eve capable of multi-user decoding is assumed in the following subsection.

A. Achievable Secrecy Rate Analysis With Single-User Decoding Eve: Upper Bound

1) Achievable Secrecy Rate Analysis for HD Communication: The achievable ergodic secrecy rate can be obtained by averaging the instantaneous secrecy rate given in Eq. (9) over the distributions of the rvs x and y, and is expressed as

$$\begin{aligned}\bar{S}_{HD} &= \mathbb{E}[S_{HD}] = \mathbb{E}[\mathcal{C}(x) - \mathcal{C}(y)]\Pr[x > y] \\ &= \log(e)\int_0^\infty \ln(1+x) f_X(x)\Pr[y < x]\,\mathrm{d}x \\ &\quad - \log(e)\int_0^\infty \ln(1+y) f_Y(y)\Pr[x > y]\,\mathrm{d}y, \end{aligned} \tag{12}$$

where $\Pr[\cdot]$ denotes probability, and $F_Y(y) \triangleq 1 - \exp(-y/\phi)$ is the CDF of Y.

The Meijer's G Function: Direct evaluation of the integrals in Eq. (12) is not straightforward. Instead, we propose to utilize the Meijer's G function, which is a highly general class of integral function that can represent a wide variety of functions and lends itself to succinct integral manipulations. The Meijer's G function, designated by the symbol $\mathrm{G}_{p,q}^{m,n}[x]$, is defined in [38, eq. (5)]. The Meijer's G function is widely adopted in the literature owing to its ease of application and readily available software implementation in standard mathematical software like Mathematica, Maple and Matlab [39].

The logarithm and the exponential function is represented in terms of the Meijer's G function as $\ln(1+x) = \mathrm{G}_{2,2}^{1,2}\left[x \middle| \begin{smallmatrix}1,1\\1,0\end{smallmatrix}\right]$ and $e^{-x} = \mathrm{G}_{0,1}^{1,0}\left[x \middle| \begin{smallmatrix}-\\0\end{smallmatrix}\right]$ [38, Eq. (11)]. Using the above representations and [40, eq. (07.34.21.0002.01)], the lower incomplete Gamma function $\gamma(m,x)$ in Eq. (3) can also be represented in terms of the Meijer's G function as $\gamma(m,x) = \int_0^x t^{m-1}\mathrm{G}_{0,1}^{1,0}\left[t \middle| \begin{smallmatrix}-\\0\end{smallmatrix}\right]\mathrm{d}t = \mathrm{G}_{1,2}^{1,1}\left[x \middle| \begin{smallmatrix}1\\m,0\end{smallmatrix}\right]$. An integration involving the product of two Meijer's G functions is also a Meijer's G function [38, eq. (21)]. The solution to integrations involving the product of three Meijer's G functions is a Meijer's G function of two variables expressed in terms of the extended generalized bivariate Meijer's G function (EGBMGF) [41, eq. (8)], [40, eq. (07.34.21.0081.01)], as presented by Eq. (13) at the bottom of this page.

Applications of the EGBMGF have been demonstrated in [42] and [43], while its efficient implementations is readily available in Mathematica [42, Table II] and Matlab [44].

Lemma 1: The achievable ergodic secrecy rate for half-duplex communication is presented in terms of the Meijer's G function and the EGBMGF as

$$\begin{aligned}\bar{S}_{HD} = \frac{\log(e)}{\Gamma(m)}\Bigg\{ &\mathrm{G}_{1,0:2,2:1,2}^{1,0:1,2:1,1}\left[\begin{smallmatrix}1\\-\end{smallmatrix}\middle|\begin{smallmatrix}1,1\\1,0\end{smallmatrix}\middle|\begin{smallmatrix}1\\m,0\end{smallmatrix}\middle|\phi, \frac{m\phi}{\mu}\right] \\ &+ \mathrm{G}_{3,2}^{1,3}\left[\frac{\mu}{m}\middle|\begin{smallmatrix}1,1,1-m\\1,0\end{smallmatrix}\right] - \Gamma(m)\mathrm{G}_{3,2}^{1,3}\left[\phi\middle|\begin{smallmatrix}1,1,0\\1,0\end{smallmatrix}\right] \\ &- \left(1+\frac{\mu}{m\phi}\right)^{-m}\mathrm{G}_{3,2}^{1,3}\left[\frac{\mu\phi}{m\phi+\mu}\middle|\begin{smallmatrix}1,1,1-m\\1,0\end{smallmatrix}\right]\Bigg\}. \end{aligned} \tag{14}$$

Proof: See Appendix A. □

2) Achievable Secrecy Rate Analysis for FD Communication: With FD communication, the total instantaneous secrecy rate of our single user system is the sum of the instantaneous secrecy rates of both the communication directions, i.e.

$$\begin{aligned}S_{FD} = &\underbrace{\max\{\log(1+\gamma_{FD}) - \log(1+\beta_a), 0\}}_{S_{FD,a}} \\ &+ \underbrace{\max\{\log(1+\gamma_{FD}) - \log(1+\beta_b), 0\}}_{S_{FD,b}}. \end{aligned} \tag{15}$$

The average of $S_{FD,a}$, the achievable secrecy rate for the Alice to Bob link, can be expanded as

$$\begin{aligned}\bar{S}_{FD,a} = &\int_0^\infty \mathcal{C}(x) f_{\gamma_{FD}}(x) F_{\beta_a}(x)\,\mathrm{d}x \\ &- \int_0^\infty \mathcal{C}(u) f_{\beta_a}(u)\left(1 - F_{\gamma_{FD}}(u)\right)\mathrm{d}u, \end{aligned} \tag{16}$$

$$\begin{aligned}&\int_0^\infty t^{\alpha-1}\mathrm{G}_{p,q}^{m,0}\left[ct\middle|\begin{smallmatrix}a_1,\ldots,a_p\\b_1,\ldots,b_q\end{smallmatrix}\right]\mathrm{G}_{p_1,q_1}^{m_1,n_1}\left[c_1 t\middle|\begin{smallmatrix}a_{11},\ldots,a_{1p_1}\\b_{11},\ldots,b_{1q_1}\end{smallmatrix}\right]\mathrm{G}_{p_2,q_2}^{m_2,n_2}\left[c_2 t\middle|\begin{smallmatrix}a_{21},\ldots,a_{2p_2}\\b_{21},\ldots,b_{2q_2}\end{smallmatrix}\right]\mathrm{d}t \\ &\qquad = c^{-\alpha}\,\mathrm{G}_{q,p:p_1,q_1:p_2,q_2}^{m,0:m_1,n_1:m_2,n_2}\left[\begin{smallmatrix}\alpha+b_1,\ldots,\alpha+b_q\\ \alpha+a_1,\ldots,\alpha+a_p\end{smallmatrix}\middle|\begin{smallmatrix}a_{11},\ldots,a_{1p_1}\\b_{11},\ldots,b_{1q_1}\end{smallmatrix}\middle|\begin{smallmatrix}a_{21},\ldots,a_{2p_2}\\b_{21},\ldots,b_{2q_2}\end{smallmatrix}\middle|\frac{c_1}{c},\frac{c_2}{c}\right]. \end{aligned} \tag{13}$$

where the PDF and CDF of γ_{FD} follows from Eqs. (2) and (3) with μ replaced by the constant $m\tilde{\mu}$ with $\tilde{\mu}$ defined as $\tilde{\mu} = \frac{\mu}{(I+1)m}$. The PDF and CDF of β_a is derived in Section II-A.

Lemma 2: The average achievable secrecy rate for the Alice to Bob link with full-duplex communication and in the presence of a SU-Eve is presented in terms of the Meijer's G function and the EGBMGF as presented by Eq. (17) at the bottom of this page.

Proof: See Appendix B. □

a) Final expression for $\bar{S}_{FD,a}$: Finally, the achievable ergodic secrecy rate for full-duplex communication in the presence of a SU-Eve is

$$\bar{S}_{FD} = \bar{S_{FD,a}} + \bar{S_{FD,b}}, \tag{18}$$

where $\bar{S}_{FD,b}$ is similarly derived as in Lemma 2 with ψ and ϕ replaced by each other.

3) Special Cases: In the special case when $\phi = \psi$, the ergodic secrecy rate with FD communication for both directions are the same, resulting in $\bar{S}_{FD} = 2\bar{S}_{FD,a} = 2\bar{S}_{FD,b}$.

Moreover, if the Alice to Bob link is assumed to be Rayleigh distributed (i.e., $m = 1$) with Eve equidistant from Alice and Bob, the ergodic secrecy rates for the HD and FD case respectively reduces to

$$\bar{S}_{HD} = \frac{\mathrm{G}_{3,2}^{1,3}\left[\mu \left| \begin{smallmatrix} 1,1,0 \\ 1,0 \end{smallmatrix} \right.\right] - \mathrm{G}_{3,2}^{1,3}\left[\frac{\mu\phi}{\mu+\phi} \left| \begin{smallmatrix} 1,1,0 \\ 1,0 \end{smallmatrix} \right.\right]}{\ln(2)}, \quad \text{and}$$

$$\bar{S}_{FD} = \frac{2\mathrm{G}_{3,2}^{1,3}\left[\tilde{\mu} \left| \begin{smallmatrix} 1,1,0 \\ 1,0 \end{smallmatrix} \right.\right]}{\ln(2)} - \frac{2\kappa \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{smallmatrix} 1 \\ - \end{smallmatrix} \middle| \begin{smallmatrix} 1,1 \\ 1,0 \end{smallmatrix} \middle| \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \middle| \kappa, \kappa\right]}{\ln(2)\tilde{\mu}} - \frac{2\kappa \sum_{\alpha=1}^{2} \phi^{\alpha-2} \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{smallmatrix} 1 \\ - \end{smallmatrix} \middle| \begin{smallmatrix} 1,1 \\ 1,0 \end{smallmatrix} \middle| \begin{smallmatrix} 1-\alpha \\ 0 \end{smallmatrix} \middle| \kappa, \kappa\right]}{\ln(2)},$$

where $\kappa = \frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi}$.

B. Achievable Secrecy Rate Analysis With Multi-User Decoding Eve

The channels from both Alice and Bob to Eve forms a multiple-access channel. In this section, Eve is assumed to be equipped with successive interference cancellation capability. In addition, we apply MAC joint decoding for the eavesdropped rate at Eve for the instances when the Alice/Bob to Eve channel is not strong enough to allow IC.

Alice and Bob are assumed to transmit to each other with fixed rates R_a and R_b respectively. IC capabilities at Eve implies it is able to decode the message from Alice/Bob if received at a rate greater than the transmission rate. Focusing on the Alice to Bob transmission link in FD mode, let us define the eavesdropped rate R_{EA} at Eve pertaining to the MAC performance with IC and JD. The eavesdropped rate measures the supremum of the achievable rate from Alice to Eve for the transmission of rate R_b by Bob. Notice that the rate R_b is not necessarily decodable by Eve. Given y, z, β_a and β_b, the eavesdropped rate is given by [32]

$$R_{EA} = \begin{cases} \mathcal{C}(y) & \text{if } R_b \le \mathcal{C}(\beta_b) \\ \mathcal{C}(y+z) - R_b & \text{if } \mathcal{C}(\beta_b) < R_b \le \mathcal{C}(z) \\ \mathcal{C}(\beta_a) & \text{if } R_b > \mathcal{C}(z), \end{cases} \tag{19}$$

where the first two cases respectively represent the eavesdropped rate following IC and JD at Eve. The secrecy rate pertaining to MAC performance is given by $S_{MAC,a} = \max(R_a - R_{EA}, 0)$. The achievable rate R_{EB} and the corresponding achievable secrecy rate for the Bob to Eve link can similarly be defined by interchanging the variables R_a with R_b, y with z, and β_a with β_b.

An analysis of the loss in achievable secrecy rate with MU-Eve compared to that with SU-Eve is presented in the following discussion. IC is investigated first, followed by MAC JD considerations at Eve. The analysis considers the Alice-Bob and Alice-Eve links. Henceforth, we assume $R_a = R_b = R$ and introduce the constant $R' = 2^R - 1$. The Alice to Bob link is assumed to support the rate R, i.e., $R \le \mathcal{C}(\gamma)$ for all channel realizations.

Successive Interference Cancellation Analysis

1) Probability of Successful IC: Let us first investigate the probabilities of successful IC at Eve. We assume perfect IC whenever possible. Eve is able to apply IC for the Bob-Eve interference channel given the rate $\mathcal{C}(\beta_b) \ge R \implies z \ge R'(y+1)$ as pictorially depicted in Figure 2a. The probability of successful IC is given by $\Pr[\text{IC}] = \Pr[z \ge R'(y+1)]$, which readily evaluates to

$$\Pr[\text{IC}] = \int_0^\infty \int_{R'(y+1)}^\infty f(z) f(y)\, \mathrm{d}z\, \mathrm{d}y = \frac{\exp(-R'/\psi)}{\phi\lambda}, \tag{20}$$

where $\lambda \triangleq \frac{R'\phi+\psi}{\phi\psi}$. It can be straightforwardly shown that the probability of successful IC approaches zero in the high SNR regime. The formal proof is omitted due to lack of space. Instead, an outline is presented below.

In the high SNR regime, ϕ and $\psi \gg 1$. Additionally, $R' \gg 1$ provided R is selected to match the channel conditions. Under normal operating conditions where ϕ and ψ are of similar order of magnitude, we thus have $\phi\lambda = 1 + \frac{R'\phi}{\psi} \gg 1$. On the other hand, the numerator in $\Pr[IC]$ is upper bounded

$$\bar{S}_{FD,a} = \frac{\log(e)}{\Gamma(m)} \left\{ \mathrm{G}_{3,2}^{1,3}\left[\tilde{\mu} \left| \begin{smallmatrix} 1,1,1-m \\ 1,0 \end{smallmatrix} \right.\right] - \left(1+\frac{\tilde{\mu}}{\phi}\right)^{-m} \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{smallmatrix} m \\ - \end{smallmatrix} \middle| \begin{smallmatrix} 1,1 \\ 1,0 \end{smallmatrix} \middle| \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \middle| \frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi}, \frac{\tilde{\mu}\psi}{\tilde{\mu}+\phi}\right] - \Gamma(m) \sum_{\alpha=1}^{2} \frac{\tilde{\mu}\psi^{\alpha-1}}{(\tilde{\mu}+\phi)} \sum_{n=0}^{m-1} \frac{\left(1+\frac{\tilde{\mu}}{\phi}\right)^{-n}}{n!} \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{smallmatrix} n+1 \\ - \end{smallmatrix} \middle| \begin{smallmatrix} 1,1 \\ 1,0 \end{smallmatrix} \middle| \begin{smallmatrix} 1-\alpha \\ 0 \end{smallmatrix} \middle| \frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi}, \frac{\tilde{\mu}\psi}{\tilde{\mu}+\phi}\right] \right\}. \tag{17}$$

by unity, i.e., $\exp(-R'/\psi) \leq 1$. Therefore, we readily observe that $\Pr[\text{IC}] \to 0$ under such conditions.

An exception can be observed when R' is low while $\psi \gg \phi$ (Eve much closer to Bob than Alice), in which case $\Pr[\text{IC}]$ will be non-negligible. However, the achievable secrecy rate defined as $(R - \mathcal{C}(y))^+$ in that case will mostly be zero owing to the fact that $y \gg 1$ following the high SNR regime assumption; and hence the impact of such successful IC on the secrecy rate is nonetheless limited.

2) Achievable Secrecy Rate Gap: Unlike the high SNR regime, the probability of successful IC is non-negligible in the SNR regime of practical interest, namely in the range of $0 \sim 30$ dB. Let us analyse the loss in the achievable secrecy rate, i.e., $\Delta S_{IC} = S_{FD,a} - s_{MAC,a}$ with IC at Eve under such circumstances. For this analysis, we further assume $R' \geq 1$, which is mostly true in the operating regime of interest. $R' < 1$ is not an interesting scenario as it leads to low secrecy rates in any case.

Assuming $R' \geq 1$, the conditions for successful IC implies non zero secrecy rate with SU-Eve, i.e. $z \geq R'(y+1) \implies y \leq R'(z+1)$. When $y \leq R'$, MU-Eve and SU-Eve both result in non zero secrecy rates, with the secrecy rate gap expressed as $\Delta S_{IC} = \mathcal{C}(y) - \mathcal{C}\left(\frac{y}{1+z}\right)$. On the other hand, $y > R'$ means zero secrecy rate with MU-Eve. Correspondingly $\Delta S_{IC} = R - \mathcal{C}\left(\frac{y}{1+z}\right)$, as shown in Figure 2a. The average secrecy rate can thus be expressed as

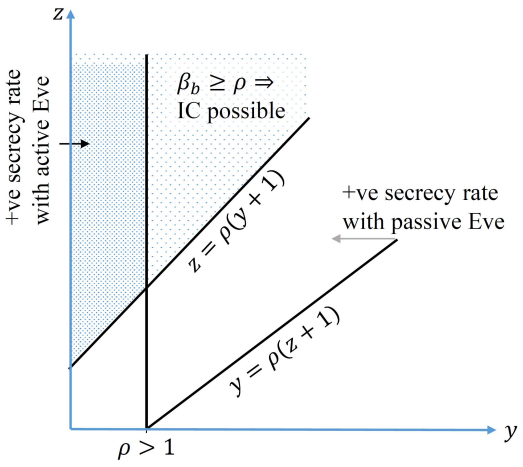
$$\begin{aligned}\Delta \bar{S}_{IC} = & \underbrace{R \int_{R'}^{\infty} \int_{R'(y+1)}^{\infty} f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y}_{L_1} \\ & + \underbrace{\int_{0}^{\infty} \int_{R'(y+1)}^{\infty} \left(\mathcal{C}(z) - \mathcal{C}(y+z)\right) f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y}_{L_2 - L_4} \\ & + \underbrace{\int_{0}^{R'} \int_{R'(y+1)}^{\infty} \mathcal{C}(y) f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y}_{L_3}. \end{aligned} \tag{21}$$

The integrals L_2, L_3 and L_4 in Eq. (21) can either be solved using the techniques outlined in Appendix VII or using suitable numerical integration techniques as outlined in [35, Ch. 25]. In order to reveal better insights, we instead propose to estimate each of these three integrals with their upper bound obtained by applying Jensen's inequality. Following some algebraic manipulation, the secrecy rate gap resulting from IC at Eve can subsequently be estimated as

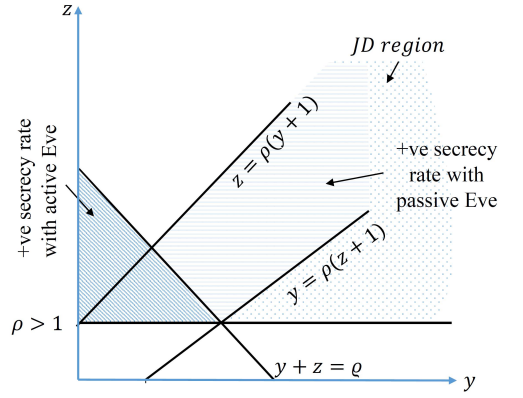
$$\Delta \bar{S}_{IC} \approx L_1 + \underbrace{\mathcal{C}\left(\hat{z}\right)}_{\geq L_2} + \underbrace{\mathcal{C}(\ddot{y})}_{\geq L_3} - \underbrace{\mathcal{C}(\hat{y} + \hat{z})}_{\geq L_4}, \tag{22}$$

where

$$\begin{aligned} L_1 &= \frac{R \exp\left(-R'\lambda + R'/\psi\right)}{\phi\lambda}, \\ \hat{y} &\triangleq \int_{0}^{\infty} \int_{R'(y+1)}^{\infty} y f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y = \frac{\exp\left(-R'/\psi\right)}{\phi\lambda^2}, \\ \ddot{y} &\triangleq \int_{0}^{R'} \int_{R'(y+1)}^{\infty} y f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y \\ &= \frac{\exp\left(-R'/\psi\right)}{\phi\lambda^2} \left[1 - (1 + \lambda R') \exp(-\lambda R')\right], \\ \hat{z} &\triangleq \int_{0}^{\infty} \int_{R'(y+1)}^{\infty} z f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y \\ &= \frac{\exp\left(-R'/\psi\right)}{\phi\lambda^2} \left[R'(1+\lambda) + \lambda\psi\right]. \end{aligned}$$



(a) IC regions of interest.



(b) JD regions of interest.

Fig. 2. Pictorial depiction of the conditions leading to a positive (+ve) secrecy rate and successful IC and MAC JD at Eve.

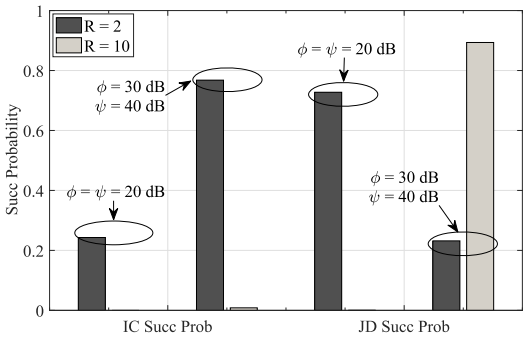
Joint Decoding Analysis

3) Probability of Successful JD: The successful JD region is characterized by the region $R' \leq z < R'(y+1)$ for all y as depicted in Figure 2b. Hence, the probability of successful JD is given by

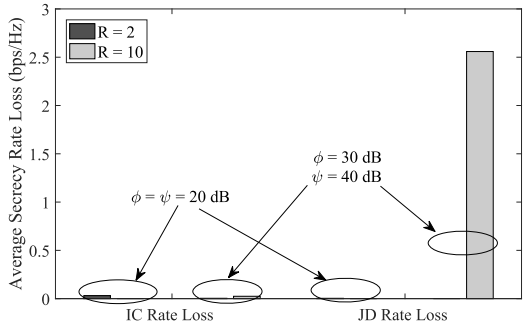
$$\Pr[\text{JD}] = \int_{0}^{\infty} \int_{R'}^{R'(y+1)} f(z) f(y) \, \mathrm{d}z \, \mathrm{d}y = \frac{R' \exp(-R'/\psi)}{\psi\lambda}. \tag{23}$$

Unlike the probability of successful IC, the probability of successful JD is not negligible under most SNR conditions.

4) Achievable Secrecy Rate Gap With JD: The gap in the achievable secrecy rate with MAC joint decoding is briefly discussed in this section. Figure 2b depicts the regions under which JD is possible and translates to a positive secrecy rate.



(a) Success Probabilities for different R values and different channel conditions.



(b) Average loss in the achievable secrecy rate with IC and JD.

Fig. 3. Numerical validation of the IC/JD success probabilities and the secrecy rate gap estimations with an IC and MAC JD capable MU-Eve.

Two different regions are of interest. Firstly, the triangular region characterized by $R' \leq z < R'(y+1)$ and $y + z \leq R'' \triangleq 2^{2R} - 1$ represents the scenario where JD is possible and results in a non-negative secrecy rate. The secrecy rate gap in this case is $R - \mathcal{C}(\beta_a) - (2R - \mathcal{C}(y+z)) = \mathcal{C}(z) - R$. The rest of the area where JD is possible pertains to zero secrecy rate following JD, in which case the secrecy rate gap is simply $R - \mathcal{C}(\beta_a)$. The ergodic secrecy rate loss resulting from MAC JD at Eve can be estimated following similar steps as in Section III-B. The straightforward derivation is omitted herein in the interest of brevity and space.

Preliminary Numerical Validation

Numerical validation of the IC/JD success probabilities and the secrecy rate gap estimations are briefly discussed in this section. The success probability with IC and MAC JD for $R = 2$ and $R = 10$ bps/Hz are shown in Figure 3a followed by the corresponding average secrecy rate gap in Figure 3b. Only the Alice to Bob link is considered. Two different channel conditions are addressed, a moderate SNR scenario of $\phi = \psi = 20$ dB and a high SNR scenario where $\phi = 30$ dB and $\psi = 40$ dB.

The probability of successful IC at Eve is found to be negligible for $R = 10$ (high R) as discussed earlier in this section. Moreover, Figure 3b reveals that the higher successful IC probability at low R translates to an negligible secrecy rate gap as indicated in the foregoing discussion. The rate loss with JD at Eve is non-negligible at higher values of R. The behaviour of this rate gap in the asymptotically high SNR regime is discussed in Section IV-C.

IV. Secrecy Degrees of Freedom Analysis

The exact secrecy capacity region is difficult to obtain under most interference conditions. The secrecy degrees of freedom, which measures the pre-log factor of the achievable secrecy rate at high SNR cases, is usually investigated instead. Though a considerably coarse measure, the sdof analysis is tractable and provides valuable insights into the secrecy capacity behaviour in the asymptotic high SNR regime.

A. Secrecy Degrees of Freedom Analysis of Half-Duplex Communication

In HD mode, the instantaneous achievable secrecy rate is given by $S_{HD} = \max\{\mathcal{C}(x) - \mathcal{C}(y), 0\}$. In the asymptotic SNR regime $\mathcal{C}(x) - \mathcal{C}(y) \to \log(\frac{x}{y})$ as $\{\mu, \phi\} \to \infty$ with fixed $\eta_\phi = \frac{\mu}{\phi}$, which in turn implies $\lim_{\{\mu,\phi\}\to\infty} S_{HD} =$

$$\lim_{\{\mu,\phi\}\to\infty} (\mathcal{C}(x) - \mathcal{C}(y)) \Pr[x > y] < \log\left(\frac{x}{y}\right).$$

Observing the rv $\frac{x}{y}$, we can deduce that $\Pr[\frac{x}{y} < \theta] = \Pr\left[y > \frac{x}{\theta}\right] = \mathbb{E}_X\left[\exp\left(-\frac{x}{\theta\phi}\right)\right]$, where the last step follows from the complimentary CDF of the exponential rv Y. The preceeding expectation is by definition the Laplace Transform (LT) of the gamma distributed rv X, and is given by $\mathcal{M}_X(s) = \mathbb{E}_X[\exp(-sx)] = \left(1 + \frac{\mu s}{m}\right)^{-m}$ [34]. Substituting the above result, we obtain $\Pr[\frac{x}{y} < \theta] = \left(1 + \frac{\eta_\phi}{m\theta}\right)^{-m}$. Using this formulation, it can be deduced that, in the asymptotic SNR regime, $\Pr[\frac{x}{y} < \infty] = 1$ as long as the ratio η_ϕ is bounded. We therefore have

$$\lim_{\{\mu,\phi\}\to\infty} S_{HD} < \infty, \tag{24}$$

i.e., the instantaneous secrecy rate with HD communication is asymptotically bounded for a bounded η_ϕ. Consequently, with a bounded instantaneous secrecy rate, the sdof of HD communication is by definition zero, i.e.

$$d_{HD} = \lim_{\mu\to\infty} \sup \frac{S_{HD}}{\log \mu} = 0. \tag{25}$$

B. Secrecy Degrees of Freedom Analysis of Full-Duplex Communication With SU-Eve

The instantaneous achievable secrecy rate in FD mode is given in terms of the SINRs γ_{FD}, β_a and β_b since $S_{FD} = \max\{\mathcal{C}\left(\gamma_{fd}\right) - \mathcal{C}\left(\beta_a\right), 0\} + \max\{\mathcal{C}\left(\gamma_{fd}\right) - \mathcal{C}\left(\beta_b\right), 0\}$. To derive the sdof, let us look into the involved SINR figures, namely γ_{FD}, β_a and β_b, in the asymptotic regime. We can observe from Eq. (7) that, by letting $\{\phi, \psi\} \to \infty$, with the ratios η_ϕ and $\eta_\psi = \frac{\mu}{\psi}$ fixed (which also implies bound $\frac{\phi}{\psi}$), the SINRs β_a and β_b remain bounded. In other words, for fixed $\frac{\phi}{\psi}$, $\Pr[\beta_a < \infty] = \Pr[\beta_b < \infty] = 1$.

On the other hand, we can rewrite the SINR of the Alice to Bob channel as $\gamma_{FD} = \frac{x}{I+1} = \frac{\mu\tilde{x}}{I+1}$, where $\tilde{x}$ is a unit mean gamma distributed rv. This allows us to present the achievable

secrecy rate $S_{FD,a}$ of the Alice to Bob link in the asymptotic SNR regime as

$$\lim_{\{\mu,\phi,\psi\}\to\infty} S_{FD,a} = \max\left\{\log(\mu)-\log\left(\frac{(1+\beta_a)(I+1)}{\tilde{x}}\right),0\right\} = \log(\mu)-\xi_a, \tag{26}$$

where $\xi_a < \infty$ is a constant. Similarly, it can be shown that the achievable secrecy rate $S_{FD,b}$ of the reverse Bob to Alice link in the asymptotic SNR regime is $\lim_{\{\mu,\phi,\psi\}\to\infty} S_{FD,b} = \log(\mu) - \xi_b$, with $\xi_b < \infty$ being a constant. Consolidating the above discussion, the sdof with FD communication with SU-Eve is expressed as $d_{FD} = \lim_{\mu\to\infty} \sup \frac{S_{FD,a} + S_{FD,b}}{\log(\mu)}$; which can be subsequently derived as

$$d_{FD} = \lim_{\mu\to\infty} \frac{2\log(\mu) - \xi_a - \xi_b}{\log(\mu)} = 2. \tag{27}$$

Hence, we can observe that the dof of FD communication is fully maintained even in the physical-layer security aspect, i.e the dof [45] and sdof in FD mode are the same. This is in contrast with conventional HD communication, where the dof is fully lost when the secrecy rate is considered [17].

C. Secrecy Degrees of Freedom Analysis of Full-Duplex Communication With MU-Eve

We have observed in Section III-B that the secrecy rate loss is negligible with interference cancellation capabilities at Eve. Hence the sdof with IC capable Eve remains unchanged. On the other hand, the rate gap with MAC joint decoding capable Eve is non-negligible. In this section, we show that this non-negligible rate gap is independent of the SNR, and hence vanishes when normalized by the $\log(SNR)$ in the asymptotically high SNR limit. Let us assume that Alice to Bob rate R is selected to support the instantaneous SNR γ, i.e., $R = \mathcal{C}(\gamma)$.

1) Probability of Positive Secrecy Rate With JD at Eve: Joint Decoding at Eve results in a positive secrecy rate when $\mathcal{C}(y+z) \leq 2R \implies y+z \leq R''$. At high SNR $R \to \log(\gamma)$, and hence $R'' = 2^{2R} - 1 \to \gamma^2$. Thus we have, $\Pr[y+z \leq R''] \to \Pr\left[\frac{\tilde{y}}{\eta_\phi} + \frac{\tilde{z}}{\eta_\psi} \leq \mu\left(\frac{\tilde{x}}{I+1}\right)^2\right]$. In the asymptotic limit as $\mu \to \infty$, this probability is one almost surely since η_ϕ, η_ψ and $\frac{\tilde{x}}{I+1}$ are bounded as $\mu \to \infty$.

2) Asymptotic Rate Gap With JD at Eve: Since, $\Pr[y+z \leq R''] \to 1$ and $R = \mathcal{C}(\gamma)$, the rate gap with JD at Eve as derived in Section III-B.2 is given by $\Delta S_{JD} = \mathcal{C}(z) - \mathcal{C}(\gamma)$. In the asymptotically high SNR limit, $\Delta S_{JD} \to \log(z/\gamma)$. As a result, we have

$$\lim_{\mu\to\infty} \frac{\Delta S_{JD}}{\log(\mu)} \to \lim_{\mu\to\infty} \frac{\log\left(\frac{\tilde{z}(I+1)}{\tilde{x}\eta_\psi}\right)}{\log(\mu)} \to 0.$$

It is thus readily observable that the rate gap with JD at Eve does not impact the sdof since it vanishes when normalized by SNR in the asymptotic SNR limit.

Hence, the secrecy degrees of freedom of full-duplex communication are unaffected in the presence of MU-Eve with interference cancellation and MAC joint decoding capabilities.

V. Applications of the Secrecy Result Findings

Applications of the derived findings in emerging 5G systems is discussed in this section.

A. Applications in Device to Device Communication

Alongside the conventional cellular connection between the base station and the user equipment, 5G systems may well support an additional device-tier architecture for direct communication among the devices. In fact, direct device-to-device (D2D) communication is envisioned as a key technology solution towards accommodating the demanding KPI targets of 5G [46]. FD communication has been proposed for such D2D communications, especially considering the close range of the devices and the symmetric nature of the traffic profile in both transmission directions [47]. FD capability is also found to allow faster device discovery for D2D nodes [48].

Security is an important technical challenges in D2D communication. Cellular networks have a certain degree of inherent security features such as authentication, integrity and access control. Due to its very nature, D2D communication cannot guarantee the same level of security as do cellular networks. The communicating parties must be assured that their data is not accessible to any unwanted nodes in the vicinity. The findings presented in this work demonstrate that a very high degree of physical-layer security can be achieved by enabling FD communication between the D2D nodes. Hence, alongside the desirable gains in terms of throughput, latency, and device discovery time, FD can also enhance physical layer security in D2D communication.

B. Applications in Cellular Networks With BS FD

Despite the potential benefits of FD communication, it may not be readily available for commercial deployment at the UE level in the recent future due to size, power, and cost constraints. An intermediate proposal is to enable the base stations with FD capabilities, and is known as the base station full-duplex (BS-FD) architecture [1].

The investigations in this contribution have revealed that the simultaneous transmission from both end of a FD communication link is the main contributor to the enhanced physical-layer security. Such a finding can be utilized to accord protection to an UE scheduled in the uplink direction with strong physical-layer security requirement in a BS-FD network.

In the downlink direction, the FD capable BS can schedule an UE in close vicinity of the uplink UE, as depicted in Figure 4. The eavesdropped signal at any eavesdropper in the vicinity of the scheduled uplink UE will be masked by the simultaneous downlink transmission to another nearby UE, thereby resulting in the strong secrecy rate demonstrated in this paper. Such interference-assisted secret communication has earlier proposed for the conventional HD network (e.g. [49, and references therein]). However, the downlink scheduled UE would also be affected by the uplink transmission. The transmission in the downlink direction must

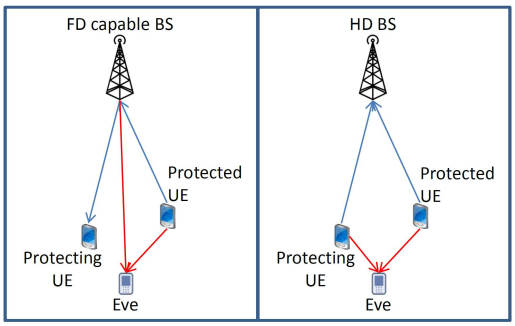


Fig. 4. Enhancing Physical-layer security though scheduling to induce a FD-like scenario at the eavesdropper node.

therefore be either *artificial noise*, or transmitted with a sufficiently low data rate. Thus, enhanced security for the BS-FD network setup is achieved at the expense of sacrificing the downlink data rate of the secondary link.

C. Applications in Conventional HD Cellular Networks

The concept of scheduling users to enhance the secrecy rate can be further extended to conventional HD networks as shown in Figure 4. An UE scheduled in the uplink direction with strong physical-layer security requirement can be concurrently scheduled with a nearby UE, also in the uplink direction. Let us term the two UEs as the *protected* and the *protecting* UE respectively. If the BS is equipped with interference cancellation or interference suppression type receivers, the traffic of both the UEs can be simultaneously decoded with a well designed radio resource management technique and/or with the aid of IC and JD at the base station. Alternatively, the *protecting* UE can be scheduled with traffic that is already known at the BS, which would make the resulting interference easily treatable.

VI. Numerical Results

The ergodic secrecy rate, the sdof and the throughput analysis of FD and HD communication are numerically validated through Matlab® based Monte Carlo simulations in this Section. At least 100, 000 independent snapshots of each scenario are simulated to ensure statistical reliability. Unless stated otherwise, the following general simulation parameters are assumed to reflect a typical propagation scenario: gamma parameter for the desired signal channel $m = 2$, the noise-normalized residual self interference $I = 1$ and Eve equidistant from Alice and Bob, i.e. $\phi = \psi$.

A. Ergodic Secrecy Rate as a Function of μ and ϕ

The ergodic secrecy rate of FD and HD communication for different ratios of the desired and eavesdropper channel SNR (i.e. $\frac{\mu}{\phi}$) with respect to (w.r.t.) the mean SNR μ are presented in Figure 5. Weak, medium, and strong eavesdropper channels are considered, corresponding to $\frac{\mu}{\phi} = [10, 0, \text{ and } -10]$ dB. First of all, FD is found to considerably enhance the physical-layer secrecy rate over conventional HD communication. This is due to the simultaneous transmission from both the transmitter and the receiver, which generates an additional source

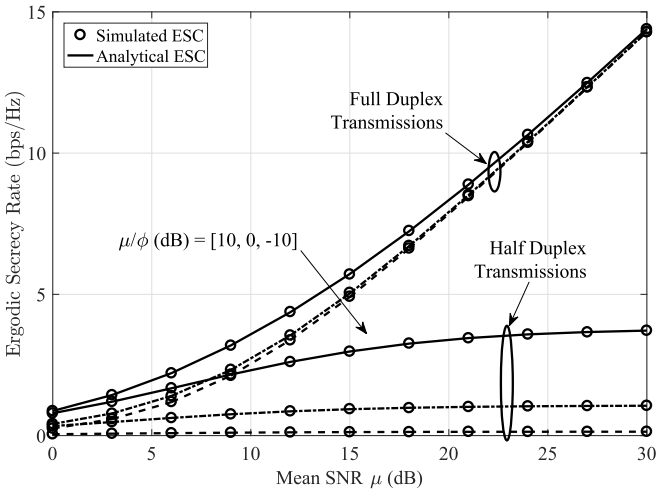


Fig. 5. The ergodic secrecy rate of FD and HD communication for different values of μ and ϕ.

of interference at the eavesdropper. The resulting interference acts as a natural deterrent to eavesdropping attempt at Eve, thereby enhancing the physical-layer security potential of FD communication.

Secondly, it is interesting to note that the ergodic secrecy rate in FD mode is almost independent of the strength towards the eavesdropper channel, especially at high SNR values. In contrast, the ergodic secrecy rate with HD is strongly dependent on the eavesdropper channel strength relative to the desired channel, and is found to approach zero for large values of $\frac{\mu}{\phi}$.

Finally, the slope of the ergodic secrecy rate curves are also distinctly different for FD and HD communication. In conventional HD mode, the ergodic secrecy rate is found to flatten out and converge to a constant as $\mu \to \infty$. On the other hand, the ergodic secrecy rate with FD communication is observed to grow linearly with a fixed slope w.r.t. μ (in dB). This confirms the analysis presented in Section IV that the sdof is 2 with FD whereas it is 0 with HD communication.

B. Ergodic Secrecy Rate as a Function of Fading Parameter m

The impact of the Gamma fading parameter m on the ergodic secrecy rate is investigated in this subsection. The ergodic secrecy rate for $m = 1$ and $m = 2.5$ with different mean SNR values w.r.t $\eta_\phi = \frac{\mu}{\phi}$ is presented in Figure 6. Gamma parameter $m = 1$ corresponds to a Rayleigh faded channel, while $m = 2.5$ reflects a channel with relatively lower amount of fading.

Similar to the findings observed in Figure 5, the ergodic secrecy rate with FD is found to be almost constant w.r.t. η_ϕ. Moreover, there is a huge gain of a factor of around 10 in the ergodic secrecy rate as μ is increased from 10 dB to 30 dB. Finally, the amount of fading is found to have only a slight impact on the ergodic secrecy rate, with the ergodic secrecy rate increasing with increasing m (i.e., as the fading gets less severe). It is worthwhile to note that the derived analytical results match perfectly with the simulation results in most

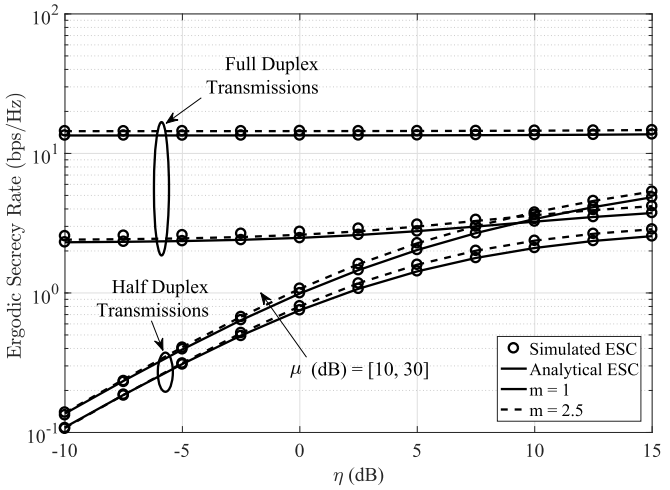


Fig. 6. The ergodic secrecy rate of FD and HD communication w.r.t. $\eta_\phi \triangleq \frac{\mu}{\phi}$ for different mean SNR (μ) and m values.

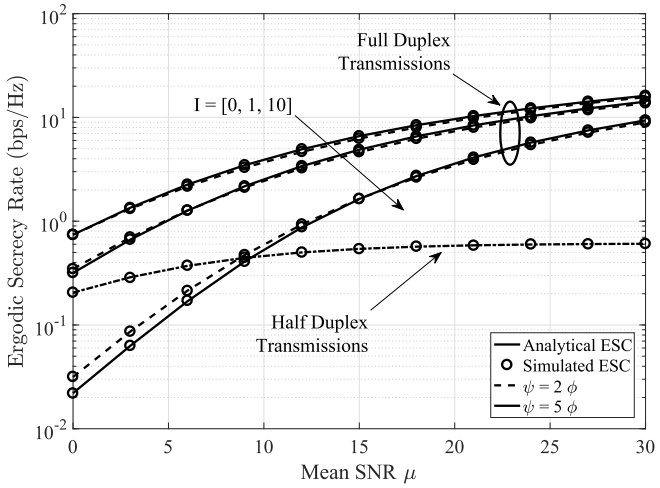


Fig. 7. The ergodic secrecy rate of FD and HD communication w.r.t. μ for different values of the self interference power I.

cases. However, since the lower incomplete gamma function was approximated by its nearest integer m for non-integer m in deriving the ergodic secrecy rate in FD mode, we can observe a slight gap for $m = 2.5$ at low η_ϕ values.

The observations for the conventional HD mode once again reveal the potential of enhancing the physical-layer security with FD communication. Firstly, the ergodic secrecy rate in HD mode is found to be strongly dependent on eavesdropper channel. Furthermore, the impact of the desired Alice to Bob channel SNR is less pronounced in this case with only a slight gain in the ergodic secrecy rate as μ is increased from 10 dB to 30 dB.

C. Ergodic Secrecy Rate as a Function of the Residual Self Interference Power I

The noise normalized residual self interference power I is an important parameter for FD communication. In this subsection, we explore its impact on the ergodic secrecy rate. The ergodic secrecy rate corresponding to perfect SIC ($I = 0$), SIC to the level of noise floor ($I = 1$) and $I = 10$ are presented w.r.t. μ in Figure 7. Furthermore, asymmetricity in the eavesdropper channel is also considered by choosing $\psi/\phi = [2, 5]$, while η_ϕ is set at 10 dB.

First of all, asymmetricity in the eavesdropper channel, i.e., having $\phi \neq \psi$, has little impact on the ergodic secrecy rate, especially at higher values of μ. In contrast, the residual self interference power plays an important role. In fact, for lower values of μ, the ergodic secrecy rate in FD mode is lower than that of HD mode with I set to 10 dB. This reiterates the well know maxim for FD communication that significant gains with FD communication requires a strong direct link (i.e., large μ) and sufficient isolation of the self interference power. Though not shown in Figure 7, the plots for different I values are found to converge to the same secrecy rate as $\mu \to \infty$, which conforms to the finding presented in Section IV that the sdof in FD mode is independent of the residual self interference power I.

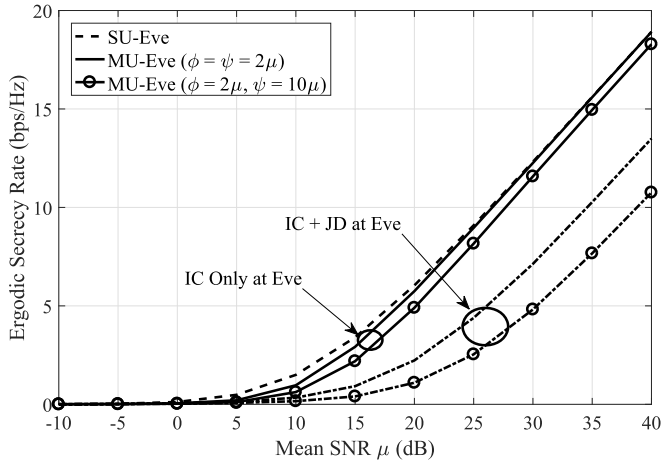


Fig. 8. The ergodic secrecy rate of FD communication with SU-Eve and MU-Eve, $I = 5$ dB.

D. Ergodic Secrecy Rate With Advanced Receiver at Eve

The ergodic secrecy rate considering a MU-Eve with successive interference cancellation and MAC joint decoding capabilities for different configurations are shown in Figure 8. Two cases are considered, namely $\phi = \psi = 2\mu$, and $\phi = 2\mu, \psi = 10\mu$. Both represent scenarios where Eve is closer to Alice/Bob than themselves - with conditions conducive for IC/JD. As discussed in Section III-B, the loss in the secrecy rate with only IC at Eve is minimal. On the other hand, that with MAC JD at Eve is not negligible, though the gap does not grow with the SNR. This is also manifested in the sdof analysis presented in Section IV-C.

E. Secrecy Degrees of Freedom Results

Being an asymptotic SNR characterization of the secrecy rate, the sdof is not readily amenable to numerical simulations. However, to demonstrate the validity of the analysis presented in Section IV, the behaviour of $\max \frac{S}{\log(\mu)}$ is presented in Figure 9 as a function of the mean SNR μ in logarithmic

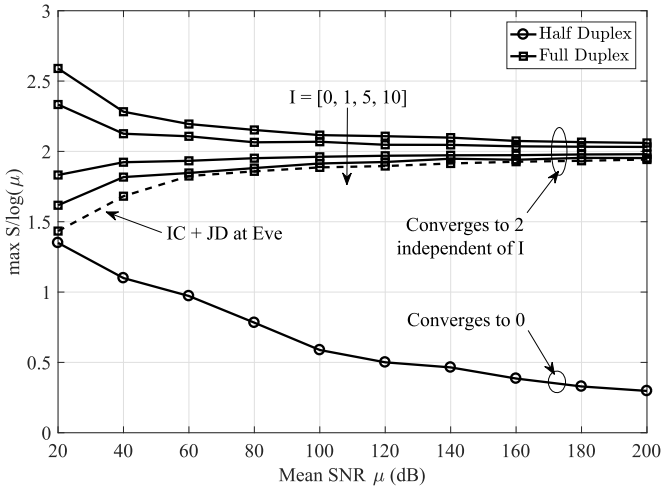


Fig. 9. The secrecy rate normalized by log of SNR in the asymptotic SNR range.

value for different values of the residual self interference power I. It is observed that as $\mu \to \infty$, the ratio of the secrecy rate over the SNR in logarithmic value converges to *two* for FD communication, even with advanced receiver at Eve (indicated by *IC + JD at Eve*). On the other hand, $\lim_{\mu\to\infty} \frac{\max S}{\log(\mu)}$ approaches *zero* in the HD mode. Hence, the reported respective sdof with FD and HD communication is clearly evident from the presented trend.

VII. Conclusions and Outlook

A thorough analysis of the potential of full-duplex communication in enhancing the physical-layer security of a wireless link is presented in this contribution. A closed form expression for the ergodic secrecy rate has been derived considering the Nakagami-m fading model. Single-user, and multi-user decoding eavesdropper with successive interference cancellation and joint decoding capabilities, are both considered. The finding is presented as a function of the eavesdropper channel strength and residual self interference power. A characterization of the secrecy rate in the asymptotic high SNR regime, namely the secrecy degrees of freedom, is also presented. Finally, comprehensive numerical results via simulations demonstrating the validity of the derived results have been presented. The analytical findings are found to closely match the simulation results in all scenarios, thereby validating the accuracy of the analysis and the presented results.

Contrary to the limited throughput gain potential, FD communication is found to provide a high degree of physical-layer security. Specifically, the ergodic secrecy rate with full-duplex communication is found to grow linearly with the log of the direct channel SNR as opposed to the flattened out secrecy rate with conventional half-duplex communication, irrespective of the eavesdropper channel strengths. Such compelling secrecy rates are found to be valid even with strong residual self interference power and under moderate SNR conditions. In fact, the sdof, i.e., the pre-log factor of the secrecy rate is found to be *two* compared to that of *zero* with conventional HD transmissions. As part of the future work, we plan to extend our study by analysing other physical-layer security metrics such as the secure outage probability and the strictly positive secrecy probability, and consider a FD Eve with active jamming capabilities.

Appendix A
Derivation of the Ergodic Secrecy Rate With HD Communication

The achievable ergodic secrecy rate given by Eq. (12) can be expanded as

$$\begin{aligned}\bar{S}_{HD} = &\underbrace{\log(e)\int_0^\infty \ln(1+x) f_X(x) F_Y(x)\,\mathrm{d}x}_{J_1} \\ &+ \underbrace{\log(e)\int_0^\infty \ln(1+y) f_Y(y) F_X(y)\,\mathrm{d}y}_{J_2} \\ &- \underbrace{\log(e)\int_0^\infty \ln(1+y) f_Y(y)\,\mathrm{d}y}_{J_3}. \end{aligned} \tag{28}$$

A. Evaluating J_1

Substituting $F_Y(y) = 1-\exp(-y/\phi)$ in Eq. (28), we obtain

$$\begin{aligned} J_1 &= \log(e)\int_0^\infty \ln(1+x)\left(1-\exp(-x/\phi)\right) f_X(x)\,\mathrm{d}x \\ &= \underbrace{\log(e)\int_0^\infty \ln(1+x) f_X(x)\,\mathrm{d}x}_{J_{11}} \\ &\quad - \underbrace{\log(e)\int_0^\infty \ln(1+x)\exp(-x/\phi) f_X(x)\,\mathrm{d}x}_{J_{12}}. \end{aligned} \tag{29}$$

Further substituting $f_X(x)$ given by Eq. (2) and isolating the integral J_{11}, we obtain

$$\begin{aligned} J_{11} &= \log(e)\int_0^\infty \ln(1+x)\frac{m^m x^{m-1}}{\mu^m \Gamma(m)}\exp\left(-\frac{mx}{\mu}\right)\mathrm{d}x \\ &= \frac{\log(e) m^m}{\mu^m\Gamma(m)}\int_0^\infty x^{m-1}\mathrm{G}_{0,1}^{1,0}\left[\frac{mx}{\mu}\,\middle|\,\begin{matrix}-\\0\end{matrix}\right]\mathrm{G}_{2,2}^{1,2}\left[x\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\right]\mathrm{d}x \\ &= \frac{\log(e)}{\Gamma(m)}\mathrm{G}_{3,2}^{1,3}\left[\frac{\mu}{m}\,\middle|\,\begin{matrix}1,1,1-m\\1,0\end{matrix}\right], \end{aligned} \tag{30}$$

where the last step is obtained following [38, eq. (21)].

Following similar steps, J_{12} in Eq. (29) is evaluated in terms of the Meijer's G function as

$$\begin{aligned} J_{12} &= \int_0^\infty \mathcal{C}(x)\frac{m^m x^{m-1}}{\mu^m\Gamma(m)}\exp\left(-\left(\frac{m}{\mu}+\frac{1}{\phi}\right)x\right)\mathrm{d}x \\ &= \frac{\left(1+\frac{\mu}{m\phi}\right)^{-m}}{\ln(2)\Gamma(m)}\mathrm{G}_{3,2}^{1,3}\left[\frac{\mu\phi}{m\phi+\mu}\,\middle|\,\begin{matrix}1,1,1-m\\1,0\end{matrix}\right]. \end{aligned} \tag{31}$$

B. Evaluating J_2

The integral J_2 in Eq. (12) can be expanded as

$$J_2 = \int_0^\infty \mathcal{C}(y)\frac{1}{\phi}\exp\left(-\frac{y}{\phi}\right)\frac{\gamma\left(m, ym/\mu\right)}{\Gamma(m)}\,\mathrm{d}y = \frac{\log(e)\int_0^\infty \mathrm{G}_{2,2}^{1,2}\left[y\left|\begin{smallmatrix}1,1\\1,0\end{smallmatrix}\right.\right]\mathrm{G}_{0,1}^{1,0}\left[\frac{y}{\phi}\left|\begin{smallmatrix}-\\0\end{smallmatrix}\right.\right]\mathrm{G}_{1,2}^{1,1}\left[\frac{my}{\mu}\left|\begin{smallmatrix}1\\m,0\end{smallmatrix}\right.\right]\mathrm{d}y}{\phi\Gamma(m)},$$

where the last step results from substituting the logarithm, the exponential and the lower incomplete gamma functions with their respective representation in terms of the Meijer's G function. The integral J_2 can be expressed in closed form in terms of the EGBMGF as

$$J_2 = \frac{\log(e)}{\Gamma(m)}\mathrm{G}_{1,0:2,2:1,2}^{1,0:1,2:1,1}\left[\begin{matrix}1\\-\end{matrix}\left|\begin{matrix}1,1\\1,0\end{matrix}\right|\begin{matrix}1\\m,0\end{matrix}\right|\phi,\frac{m\phi}{\mu}\Bigg]. \quad (32)$$

C. Evaluating J_3

The last integral J_3 in Eq. (28), which reads $J_3 = \frac{\log(e)}{\phi}\int_0^\infty \ln(1+y)\exp\left(-y/\phi\right)$ can be solved following similar steps as in Eq. (30) by substituting $m = 1$ and $\mu = \phi$. The resulting expression for J_3 is

$$J_3 = \log(e)\mathrm{G}_{3,2}^{1,3}\left[\phi\left|\begin{matrix}1,1,0\\1,0\end{matrix}\right.\right]. \quad (33)$$

Appendix B
Derivation of the Ergodic Secrecy Rate With FD Communication

The average achievable secrecy rate of the Alice to Bob link in FD mode given by Eq. (16) can be expressed as a sum of integrals as follows

$$\bar{S}_{FD,a} = \underbrace{\int_0^\infty \mathcal{C}(x) f_{\gamma_{FD}}(x) F_{\beta_a}(x)\,\mathrm{d}x}_{K_1} + \underbrace{\int_0^\infty \mathcal{C}(u) f_{\beta_a}(u) F_{\gamma_{FD}}(u)\,\mathrm{d}u}_{K_2} - \underbrace{\int_0^\infty \mathcal{C}(u) f_{\beta_a}(u)\,\mathrm{d}u}_{K_3}. \quad (34)$$

D. Evaluating K_1

Using Eqs. (2) and (7), the integral K_1 in Eq. (16) can be expanded as

$$K_1 = \underbrace{\int_0^\infty \mathcal{C}(x) f_{\gamma_{FD}}(x)\,\mathrm{d}x}_{K_{11}} - \underbrace{\int_0^\infty \mathcal{C}(x) e^{\left(-\frac{x}{\phi}\right)}\left(1+\frac{x\psi}{\phi}\right)^{-1} f_{\gamma_{FD}}(x)\,\mathrm{d}x}_{K_{12}}. \quad (35)$$

Following the steps involved in evaluating J_{11}, we have

$$K_{11} = \frac{\log(e)}{\Gamma(m)}\mathrm{G}_{3,2}^{1,3}\left[\tilde{\mu}\left|\begin{matrix}1,1,1-m\\1,0\end{matrix}\right.\right]. \quad (36)$$

On the other hand, the second integral K_{12} can be expanded as an integration involving a product of three Meijer's G functions; with a close form solution in terms of the EGBMGF defined in Eq. (13) as follows

$$K_{12} = \int_0^\infty \frac{x^{m-1}\exp\left(-\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)x\right)\ln(1+x)}{\ln(2)\tilde{\mu}^m\Gamma(m)\left(1+\frac{\psi}{\phi}x\right)}\,\mathrm{d}x = \int_0^\infty \frac{\mathrm{G}_{0,1}^{1,0}\left[\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)x\left|\begin{smallmatrix}-\\0\end{smallmatrix}\right.\right]\mathrm{G}_{2,2}^{1,2}\left[x\left|\begin{smallmatrix}1,1\\1,0\end{smallmatrix}\right.\right]\mathrm{G}_{1,1}^{1,1}\left[\frac{\psi}{\phi}x\left|\begin{smallmatrix}0\\0\end{smallmatrix}\right.\right]}{\ln(2)\tilde{\mu}^m\Gamma(m)x^{1-m}}\,\mathrm{d}x = \frac{\left(1+\frac{\tilde{\mu}}{\phi}\right)^{-m}\mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{matrix}m\\-\end{matrix}\left|\begin{matrix}1,1\\1,0\end{matrix}\right|\begin{matrix}0\\0\end{matrix}\right|\frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi},\frac{\tilde{\mu}\psi}{\tilde{\mu}+\phi}\Bigg]}{\ln(2)\Gamma(m)}, \quad (37)$$

where the second step follows from the relation $(1+cx)^\alpha = \frac{1}{\Gamma(-\alpha)}\mathrm{G}_{1,1}^{1,1}\left[cx\left|\begin{smallmatrix}\alpha+1\\0\end{smallmatrix}\right.\right]$ [38, eq. (10)].

E. Evaluating K_2

Substituting the respective gamma CDF and the PDF of the SINR β at Eve from Eq. (6), the integral K_2 is expanded as a product of four distinct terms that can be represented as four different Meijer's G functions. However, an integration involving four terms of Meijer's G function is not readily solvable. To overcome this limitation, we proposed to restrict the gamma parameter m to be a an integer. Please note, the solution in the case of a non-integer m value can be approximated by replacing m with its closest integer. In that case, we can represent the CDF of γ_{FD} using the recurrence relation $\gamma\left(m+1,x\right) = m\gamma\left(m,x\right) - x^m\exp(-x)$ for integer positive m as $\gamma\left(m,x\right) = \Gamma(m)\left(1-\exp\left(-x\right)\sum_{n=0}^{m-1}\frac{x^n}{n!}\right)$ [35, eq. (6.5.13)]. Subsequently, the integral K_2 is solved as

$$K_2 = \int_0^\infty \mathcal{C}(u)\left(1-\exp\left(-\frac{u}{\tilde{\mu}}\right)\sum_{n=0}^{m-1}\frac{u^n}{\tilde{\mu}^n n!}\right)f_{\beta_a}(u)\,\mathrm{d}u = K_3 - K_2', \quad (38)$$

where

$$K_2' = \sum_{\alpha=1}^{2}\frac{\psi^\alpha}{\psi\phi}\sum_{n=0}^{m-1}\frac{\tilde{\mu}^{-n}}{n!}\int_0^\infty \frac{u^n\ln(1+u)\left(1+\frac{\psi}{\phi}u\right)^{-\alpha}}{\exp\left(\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)u\right)}\,\mathrm{d}u = \sum_{\alpha=1}^{2}\frac{\psi^{\alpha-1}}{\phi}\sum_{n=0}^{m-1}\frac{1}{\tilde{\mu}^n n!}\int_0^\infty u^n\mathrm{G}_{0,1}^{1,0}\left[\left(\frac{1}{\tilde{\mu}}+\frac{1}{\phi}\right)u\left|\begin{smallmatrix}-\\0\end{smallmatrix}\right.\right] \times \mathrm{G}_{2,2}^{1,2}\left[u\left|\begin{smallmatrix}1,1\\1,0\end{smallmatrix}\right.\right]\mathrm{G}_{1,1}^{1,1}\left[\frac{\psi}{\phi}u\left|\begin{smallmatrix}1-\alpha\\0\end{smallmatrix}\right.\right]\mathrm{d}u = \sum_{\alpha=1}^{2}\frac{\tilde{\mu}\psi^{\alpha-1}}{\ln(2)(\tilde{\mu}+\phi)}\sum_{n=0}^{m-1}\frac{\left(1+\frac{\tilde{\mu}}{\phi}\right)^{-n}}{n!} \times \mathrm{G}_{1,0:2,2:1,1}^{1,0:1,2:1,1}\left[\begin{matrix}n+1\\-\end{matrix}\left|\begin{matrix}1,1\\1,0\end{matrix}\right|\begin{matrix}1-\alpha\\0\end{matrix}\right|\frac{\tilde{\mu}\phi}{\tilde{\mu}+\phi},\frac{\tilde{\mu}\psi}{\tilde{\mu}+\phi}\Bigg]. \quad (39)$$

Substituting K_1 and K_2 into Eq. (34) yields the final expression for $\bar{S}_{FD,a}$ in Eq. (17).

ACKNOWLEDGMENT

The authors would like to thank the editor and the anonymous reviewers for their valuable suggestions, time and efforts during the review process; and graciously acknowledge the support of their colleague Mads Lauridsen for reviewing the manuscript. The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] A. Sabharwal, P. Schniter, D. Guo, D. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[2] S. Hong *et al.*, "Applications of self-interference cancellation in 5G and beyond," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

[3] N. H. Mahmood, G. Berardinelli, F. M. L. Tavares, and P. Mogensen, "On the potential of full duplex communication in 5G small cell networks," in *Proc. IEEE 81st VTC Spring*, Glasgow, U.K., May 2015, pp. 1–5.

[4] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 680–694, Feb. 2014.

[5] S. Goyal, P. Liu, S.Panwar, R. A. DiFazio, R. Yang, and E. Bala, "Full duplex cellular systems: will doubling interference prevent doubling capacity," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 121–127, May 2015.

[6] X. Xie and X. Zhang, "Does full-duplex double the capacity of wireless networks?" in *Proc. The 33rd INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 253–261.

[7] Z. Tong and M. Haenggi, "Throughput analysis for wireless networks with full-duplex radios," in *Proc. WCNC*, New Orleans, LA, USA, Mar. 2015, pp. 717–722.

[8] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.

[9] S. Talwar, D. Choudhury, K. Dimou, E. Aryafar, B. Bangerter, and K. Stewart, "Enabling technologies and architectures for 5G wireless," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Tampa, FL, USA, Jun. 2014, pp. 1–4.

[10] M. G. Sarret, G. Berardinelli, N. H. Mahmood, M. Fleischer, P. E. Mogensen, and H. Heinz, "Analyzing the potential of full duplex in 5G ultra-dense small cell networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, p. 284, Dec. 2016.

[11] N. H. Mahmood, M. G. Sarret, G. Berardinelli, and P. Mogensen, "Full duplex communications in 5G small cells," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Valencia, Spain, Jun. 2017.

[12] M. Cai, Q. Liu, H. Jiang, P. Cao, and C. Hong, "A 15GHz full duplex system for microwave backhauling," in *Proc. IEEE 81st VTC Spring*, Glasgow, U.K., May 2015, pp. 1–5.

[13] H. Tabassum, A. H. Sakr, and E. Hossain, "Analysis of massive MIMO-enabled downlink wireless backhauling for full-duplex small cells," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2354–2369, Jun. 2016.

[14] W. Shin, N. Lee, H. Yang, and J. Lee, "Relay-aided successive aligned interference cancellation for wireless X networks with full-duplex relays," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 421–432, Jan. 2017.

[15] Z. Zhang, Z. Ma, M. Xiao, G. K. Karagiannidis, Z. Ding, and P. Fan, "Two-timeslot two-way full-duplex relaying for 5G wireless communication networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2873–2887, Jul. 2016.

[16] M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng, and I. Krikidis, "Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1769–1785, Apr. 2016.

[17] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[18] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[19] H. Alves, G. Brante, R. D. Souza, D. B. da Costa, and M. Latva-Aho, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 867–870, Jul. 2015.

[20] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[21] H. He, P. Ren, Q. Du, and L. Sun, "Full-duplex or half-duplex? Hybrid relay selection for physical layer secrecy," in *Proc. IEEE 83rd VTC Spring*, Nanjing, China, May 2016, pp. 1–5.

[22] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[23] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[24] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[25] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[26] Ö. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1075–1078, Jun. 2014.

[27] O. Taghizadeh, A. Zamani, and R. Mathar, "Physical-layer security for simultaneous information and power transfer in full-duplex multi-user networks," in *Proc. 20th Int. ITG Workshop Smart Antennas (WSA)*, Mar. 2016, pp. 1–8.

[28] J. Zhang, G. Pan, and H.-M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, Jul. 2016.

[29] S. Vishwakarma and A. Chockalingam. (2014). "Sum secrecy rate in full-duplex wiretap channel with imperfect CSI." [Online]. Available: https://arxiv.org/abs/1311.3918

[30] N. H. Mahmood, I. S. Ansari, P. E. Mogensen, and K. A. Qaraqe, "On the ergodic secrecy capacity with full duplex communication," in *Proc. IEEE ICC*, Paris, France, May 2017, pp. 2281–2286.

[31] N. H. Mahmood, P. Popovski, I. S. Ansari, P. E. Mogensen, and K. A. Qaraqe, "Physical-layer security potential of full-duplex communication with multiuser receiver at eve," in *Proc. IEEE Globecom*, submitted for publication.

[32] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 2, pp. 242–256, Jun. 2009.

[33] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[34] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*, 2nd ed. Hoboken, NJ, USA: Wiley, Dec. 2005.

[35] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: National Bureau of Standards, 1964.

[36] U. Niesen and M. A. Maddah-Ali, "Interference alignment: From degrees of freedom to constant-gap capacity approximations," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4855–4888, Aug. 2013.

[37] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with arbitrarily varying eavesdropper channel: Secrecy degrees of freedom," in *Proc. IEEE GLOBECOM*, Houston, TX, USA, Dec. 2011, pp. 1–5.

[38] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," in *Proc. Int. Symp. Symbolic Algebraic Comput. (ISSAC)*, New York, NY, USA, Jul. 1990, pp. 212–224.

[39] B. Oreshkin. *MeijerG: Implements Meijer G-Function Using Interface With MuPAD*, accessed on Aug. 22, 2016. [Online]. Available: https://se.mathworks.com/matlabcentral/fileexchange/31490-meijerg

[40] Wolfram. *The Wolfram Functions Site*, accessed on Aug. 15, 2016. [Online]. Available: http://functions.wolfram.com/

[41] S. C. Gupta, "Integrals involving products of G-function," *Proc. Natural Acad. Sci., India*, vol. 39(A), no. 2, Apr. 1969.

[42] I. S. Ansari, S. Al-Ahmadi, F. Yilmaz, M. S. Alouini, and H. Yanikomeroglu, "A new formula for the BER of binary modulations with dual-branch selection over generalized-K composite fading channels," *IEEE Trans. Commun.*, vol. 59, no. 10, pp. 2654–2658, Oct. 2011.

[43] K. P. Peppas, "A new formula for the average bit error probability of dual-hop amplify-and-forward relaying systems over generalized shadowed fading channels," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 85–88, Apr. 2012.

[44] H. Chergui, M. Benjillali, and S. Saoudi, "Performance analysis of project-and-forward relaying in mixed MIMO-pinhole and Rayleigh dual-hop channel," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 610–613, Mar. 2016.
[45] N. H. Mahmood, I. S. Ansari, G. Berardinelli, P. Mogensen, and K. A. Qaraqe, "Analysing self interference cancellation in full duplex radios," in *Proc. IEEE WCNC*, Doha, Qatar, Apr. 2016, pp. 1–6.
[46] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, May 2014.
[47] E. Hossain and M. Hasan, "5G cellular: Key enabling technologies and research challenges," *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, Jun. 2015.
[48] M. G. Sarret, G. Berardinelli, N. H. Mahmood, B. Soret, and P. Mogensen, "Can full duplex reduce the discovery time in D2D communication?" in *Proc. IEEE 13th ISWCS*, Poznan, Poland, Sep. 2016, pp. 27–31.
[49] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secrect communication," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Porto, Portugal, May 2008, pp. 164–168.

Nurul Huda Mahmood (S'06–M'13) was born in Chittagong, Bangladesh. He received the M.Sc. degree in mobile communications from Aalborg University (AAU), Denmark, in 2007, and the Ph.D. degree in wireless communications from the Norwegian University of Science and Technology, Norway, in 2012. He has been with the Wireless Communication Networks Section, AAU, since 2012. He is also contributing to the EU funded research project FANTASTIC-5G. He has authored/co-authored over 40 peer-reviewed publications. His current research interests include resource optimization techniques, modeling and performance analysis of wireless communication systems, and full duplex communication.

Imran Shafique Ansari (S'07–M'15) received the B.Sc. degree (Hons.) in computer engineering from the King Fahd University of Petroleum and Minerals in 2009, and the M.Sc. and Ph.D. degrees from the King Abdullah University of Science and Technology (KAUST), in 2010 and 2015, respectively.

In 2009, he was a Visiting Scholar with Michigan State University, East Lansing, MI, USA, and in 2010, he was a Research Intern with Carleton University, Ottawa, ON, Canada. He is currently a Post-Doctoral Research Associate with Texas A&M University at Qatar (TAMUQ). He has authored or co-authored 50+ journal and conference publications. He has co-organized the GRASNET'2016, 2017 workshops in conjunction with the IEEE WCNC'2016, 2017. His current research interests include free-space optics, channel modeling/signal propagation issues, relay/multihop communications, physical layer secrecy issues, full duplex systems, and diversity reception techniques among others.

Dr. Ansari has been affiliated with the IEEE and IET since 2007 and has served in various capacities. He has been serving on the IEEE Communication Society Young Professionals (ComSoc YP) Board, since 2016. He has been a part of the IEEE 5G Tech Focus Publications Editorial Board since 2017. He has served on the IET CC-EMEA (Communities Committee–Europe, Middle-East, and Africa) for a complete term from 2010 to 2013 and has been re-elected to serve for another term from 2015 to 2018. He is serving on the IET Satellite and Systems Applications Technical Professional Network from 2016–2019. He is an Active Reviewer for various IEEE TRANSACTIONS and various other journals. He has served as a TPC for various IEEE conferences. He is a recipient of appreciation for an Exemplary Reviewer of the IEEE TRANSACTION ON COMMUNICATIONS in 2016, a recipient of TAMUQ Research Excellence Award 2016 and 2017, a recipient of the Recognized Reviewer Certificate by Elsevier Optics Communications in 2015, a recipient of the Recognized Reviewer Certificate by OSA Publishing in 2014, a recipient of appreciation for an Exemplary Reviewer of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, a recipient of the Post-Doctoral Research Award (first cycle) with the Qatar National Research Foundation in 2014, a recipient of the KAUST Academic Excellence Award in 2014, and a recipient of the IEEE Richard E. Merwin Student Scholarship Award in 2013.

Petar Popovski (S'97–A'98–M'04–SM'10–F'16) received the Dipl.Ing. degree in electrical engineering and the Magister Ing. degree in communication engineering from the Saints Cyril and Methodius University of Skopje, Skopje, Macedonia, in 1997 and 2000, respectively, and the Ph.D. degree from Aalborg University, Denmark, in 2004. He is currently a Professor of Wireless Communications with Aalborg University. He has authored or co-authored over 290 publications in journals, conference proceedings, and books. He holds over 30 patents and patent applications. His research interests include wireless communication and networking, and communication/information theory. He is currently a Steering Committee Member of the IEEE SmartGridComm and previously served as a Steering Committee Member of the IEEE INTERNET OF THINGS JOURNAL. He is a holder of a Consolidator Grant from the European Research Council, a recipient of the Danish Elite Researcher Award and a member of the Danish Academy for Technical Sciences. He is currently an Area Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Preben Mogensen received the M.Sc. and Ph.D. degrees from Aalborg University in 1988 and 1996, respectively. Since 1995, he has also been with Nokia (part time), and was nominated an NSN Fellow in 2009. He became a Full Professor with Aalborg University in 1999, and currently heads the Wireless Communication Networks Section, Department of Electronic Systems. He has supervised over 35 successfully finalized Ph.D. candidates and has co-authored over 300 scientific publications His current research is on 5G and IoT.

Khalid A. Qaraqe (SM'00) was born in Bethlehem. He received the B.S. degree (Hons.) from the University of Technology, Bagdad, Iraq, in 1986, the M.S. degree from the University of Jordan, Jordan, Jordan, in 1989, and the Ph.D. degree from Texas A&M University, College Station, TX, USA, in 1997, all in electrical engineering. From 1989 to 2004, he has held a variety of positions in many companies and he has over 12 years of experience in the telecommunication industry. He was involved in numerous GSM, CDMA, and WCDMA projects and has experience in product development, design, deployments, testing and integration. He joined the Department of Electrical and Computer Engineering, Texas A&M University at Qatar, in 2004, where he is currently a Professor.

His research interests include communication theory and its application to design and performance, and the analysis of cellular systems and indoor communication systems. His particular interests include mobile networks, broadband wireless access, cooperative networks, cognitive radio, diversity techniques, and 5G systems.